MANUAL

DRAFT – 0
DOE M XXX.X-X

Approved: XX-XX-06
Expires: XX-XX-09

DEPARTMENT OF ENERGY ELECTRONIC RECORDS MANAGEMENT MANUAL

U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

AVAILABLE ONLINE AT:
http://www.directives.doe.gov

INITIATED BY:
Office of Chief Information Officer

1. PURPOSE. This Department of Energy (DOE) Manual provides detailed requirements to supplement DOE O 243.1, *Records Management*, and dated 02-03-06. Implementing the requirements of this manual will:

   a. Ensure that all DOE electronic records are managed in accordance with the Federal Records Act [Public Law (P.L.) 81-574] ,

   b. Facilitate the implementation of the E-Government Act of 2002, and

   c. Ensure electronic records are reliable, authentic, trustworthy, and usable.

   Reliability means the electronic records can be trusted as accurate; authentic means the records are complete and acceptable as a record; trustworthy means the records have not been altered after completion; and usability means electronic records can be easily located and retrieved by those with a need for the information.

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. All Departmental Elements. Except for the exclusions in paragraph 3c, this Manual applies to all departmental elements (see Attachment 1 for a complete list of all departmental elements). This Manual automatically applies to departmental elements created after it is issued.

   The Administrator of the National Nuclear Security Administration (NNSA) will assure that NNSA employees and contractors comply with their respective responsibilities under this Manual.

   b. DOE Contractors. Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements to be applied to contractors that create, receive, use, maintain, disseminate, and/or dispose of DOE records in connection with the performance of DOE-funded tasks or activities.

      (1) The Contractor Requirements Document, Attachment 2, sets forth requirements of this Manual that will apply to site/facility management contractors. Contractor compliance with the CRD will be required to the extent set forth in a contract.

      (2) The CRD must be included in site/facility management contracts that may involve the receipt, creation, use, maintenance, dissemination and/or disposition of DOE records.

      (3) The office identified in the responsibilities paragraph in DOE O 243.1, section 5.c is responsible for notifying the contracting officer of which site/facility

management contracts are affected. Once notified, the contracting officer is responsible for incorporating the CRD into the laws, regulations, and DOE directives clause of each affected site/facility management contract.

(4) As the laws, regulations, and DOE directives clause of a site/facility management contract states, regardless of the performer of the work, the site/facility management contractor with the CRD incorporated into its contract is responsible for compliance with the requirements of the CRD.

(5) An affected site/facility management contractor is responsible for flowing down the requirements of the CRD to subcontractors at any tier to the extent necessary to ensure the site/facility management contractor's compliance with the requirements.

c. Exclusions. In accordance with the responsibilities and authorities assigned by Executive Order 12344 and to ensure consistency throughout the joint Navy and DOE organization of the Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors will implement and oversee all requirements and practices pertaining to this DOE Manual for activities under the Deputy Administrator's cognizance.

4. SUMMARY. This Manual is composed of ten chapters that provide direction for managing electronic records. These chapters address mandatory procedures and management processes. Chapter I describes the responsibilities of the positions directly involved in managing electronic records. Chapters II through IV describe the requirements for all Electronic Records, and Chapters V through X address special categories or formats of electronic records; specifically Electronic Information Systems, Electronic Mail Records, Web Records, Vital Records, Permanent Electronic Records, and Imaging Systems. Attachment 1 lists the organizations to which this Manual applies, and Attachment 2 contains the Contractor Requirements Document.

5. DEFINITIONS.

a. DATA BASE. A set of data, consisting of at least one data file, that is sufficient for a given purpose.

b. DATE BASE MANAGEMENT. A software system used to access and retrieve records/data stored in a data base.

c. DATA FILE. Related numeric, textual, or graphic information that is organized in a strictly prescribed form and format.

d. ELECTRONIC INFORMATION SYSTEM. A system that contains and provides access to computerized Federal records and other information.

e. ELECTRONIC MAIL SYSTEM. A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer

utilities (software that transmits files between users but does not retain any transmission data), systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, files or data bases on either personal computers or mainframe computers, and word processing documents not transmitted on an e-mail system.

f. ELECTRONIC MAIL MESSAGE. A document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.

g. ELECTRONIC RECORD. Any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record.

h. ELECTRONIC RECORDS MANAGEMENT. Electronic records management is using automated techniques to manage records regardless of format or media. Electronic records management is the broadest term that refers to electronically managing records on varied media (e.g., paper, microform, video, etc). Electronic recordkeeping is a subset of electronic records management because electronic recordkeeping focuses on electronically managing records.

i. ELECTRONIC RECORDKEEPING. Electronic recordkeeping is the development of automated processes an agency uses to manage its electronic records. These automated processes support not only the preservation of an electronic record's content, but also its context and structure over time.

j. RECORDS. All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that Agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them (44 U.S.C. 3301). [DOE 243.1]

k. RECORDS DISPOSITION SCHEDULE. A document providing mandatory instructions for what to do with records (and nonrecord materials) no longer needed for current Government business, with provision of authority for the final disposition of recurring or nonrecurring records. Also called records disposition schedule, records retention schedule, records control schedule, or schedule.

l. TEXT DOCUMENTS. Narrative or tabular documents, such as letters, memorandums, and reports in loosely prescribed form and format.

m. TRANSMISSION AND RECEIPT DATA.

(1) Transmission Data. Information in electronic mail systems regarding the identities of the sender and addressee(s), and the data and time messages were sent.

(2) Receipt Data. Information in electronic mail systems regarding date and time of receipt of a message, and/or acknowledgement of receipt or access by addressee(s).

6. REFERENCES. In addition to references cited in the Manual:

a. DOE O 243.1, *Records Management Program*, dated 2-3-06

b. DOE O 243.2, *Vital Records*, dated 2-2-06

c. DOE O 420.1A, *Facility Safety*, dated 5-20-02.

d. DOE O 470.1, *Safeguards and Security Program*, dated 9-28-95.

e. DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.

f. DOE O 471.2A, *Information Security Program*, dated 3-27-97.Public Law (P.L.) 106-65, National Nuclear Security Administration Act of 1999, as amended, which establishes NNSA as a separately organized agency within DOE (www.nnsa.doe.gov/).

g. DOE CIO Guidance CS-38, *Protection of Personally Identifiable Information* dated 7-20-2006.

h. P.L. 104-201, Section 3174, National Defense Authorization Act for FY 1997, which requires findings before imposing any DOE Orders at a defense nuclear facility

i. 36 CFR 1234, which establishes the basic requirements related to the creation, maintenance, use, and disposition of electronic records.

7. CONTACT. Questions concerning this Manual should be addressed to the Office of the Chief Information Officer at 301-903-3455.

SAMUEL W. BODMAN
Secretary of Energy

CONTENTS

CONTENTS (continued)

CHAPTER I. RESPONSIBILITIES

1. Electronic system owners are responsible for:

   a. Ensuring the value of the system and its data has been evaluated and scheduled for disposition in a NARA-approved records disposition schedule.

   b. Coordinating the disposition of the system and its data with the appropriate Program Records Official, Records Management Field Officers, or Records Liaison Officer.

   c. Adequately addressing retention and maintenance issues and ensuring the system is not rolled over, decommissioned, or migrated without the concurrence of the Program Records Official or Departmental Records Officer.

   d. Scheduling disposition of electronic records during the Capital Planning and Investment Control (CPIC) process, but no later than one year, after implementation of the system.

2. System developers are responsible for:

   a. Ensuring incorporation of records management and archival functions into the design, development, and implementation of the information system [OBM-130, 8.k] by including the appropriate Program Records Official, Records Liaison Officer, or Field Records Officer.

   b. Developing and maintaining up-to-date documentation about the electronic information system that is adequate to: Specify all technical characteristics necessary for reading or processing the records; identify all defined inputs and outputs of the system; define the contents of the files and records; determine restrictions on access and use; understand the purpose(s) and function(s) of the system; describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and ensuring the timely, authorized disposition of the record. [36 CFR 1234.10 (g)].

3. The Office of the Chief Information Officer is responsible for:

   a. Specifying the location, manner, and media in which electronic records will be maintained to meet operational and archival requirements, and maintaining up-to-date inventories of electronic information systems to facilitate disposition. Maintaining an up-to-date inventory of all electronic information systems [36 CFR 1234.10, (h)], and making the inventory information available to the PRO's on an annual basis. At a

minimum, this inventory should contain the system name, system owner, and purpose of the system.

b. Ensuring adequate training is provided for users of electronic mail systems on recordkeeping requirements, the distinction between Federal records and nonrecord materials, procedures for designating Federal records, and moving or copying records for inclusion in an organization's recordkeeping system. [36 CFR 1234.10 (e)]

c. Reviewing electronic information systems periodically for conformance to established agency procedures, standards, and policies as part of the periodic reviews required by 44 U.S.C. 3506. The review should determine if the records have been properly identified and described, and whether the schedule descriptions and retention periods reflect the current informational content and use. If not, or if substantive changes have been made in the structure, design, codes, purposes, or use of the system, submit an SF 115, Request for Records Disposition Authority, to the Departmental Records Manager. [36 CFR 1234.10 (m)].

d. Reviewing proposed new information systems through the Capital Planning and Investment Control (CPIC) process for records management implications to ensure records created by the new system, as well as system documentation, are appropriately identified and scheduled.

e. Integrating the management of electronic records with other records and information resources management programs of the agency. [36 CFR 1234.10 (b)].

4. Program Records Officials, Records Liaison Officers, and Records Management Field Officers are responsible for:

a. Developing appropriate procedures to ensure implementation of the Electronic Records Management Manual.

b. Assessing electronic records management under their cognizance at least every 3 years.

5. Departmental Records Officer

a. Establishing and disseminating electronic records management policies, objectives, and guidance in accordance with regulatory requirements and NARA guidance.

b. Reviewing OMB Exhibit 300's to ensure the records/data are managed properly and the records and system documentation have been appropropriately scheduled..

c. Developing and securing NARA approval of records disposition schedules, and ensuring implementation of their provisions. [36 CFR 1234.10 (i)]

6. Capital Planning and Investment Control Program Manager

a. Establishing procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic systems or enhancements to existing systems. [36 CFR 1234.10 (d)]

b. Ensuring the OMB 300 process provides adequate interface with the Departmental Records Officer and the appropriate PRO, RMFO, or RLO.

7. Systems Security Manager

a. Specifying the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically. [36 CFR 1234.10 (d)]

b. Ensuring systems and their data have NARA-approved retention schedules before certifying a system as operational.

CHAPTER II. GENERAL REQUIREMENTS

1. INTRODUCTION. Electronic records (ER), as defined by the National Archives and Records Administration (NARA) means any information that is recorded in a form that only a computer can process **and** that satisfies the definition of a Federal record per the Federal Records Act. At its most basic level, an electronic record is:

   a. Documentary material in any format or media (e.g., database, text document, compact disk) that is created or received in the course of activities as a DOE employee or contractor, and

   b. Warrants preservation because of the value of the information in them, and

   c. Requires an electronic device such as a computer to process it.

   The creation, maintenance, use and disposition of records frequently takes place using purely electronic processes. In other instances, paper text documents are converted to an electronic media and managed electronically upon verification of accurate conversation. Electronic records, like their paper counterparts, must be actively managed to ensure they are authentic, reliable, and are accessible to those who need them, when they need them. Processes must be in place to ensure that electronic records are created, maintained, and disposed of according to all applicable business and regulatory requirements.

2. BACKGROUND.

   In brief, Records Management (RM) is the "umbrella term" used for the general management of all records, with electronic forming a significant and ever increasing component. A utilized element of RM has been the application of automated management of electronic records from creation through disposition and referred to as an electronic recordkeeping system (ERKS). An EKRS may also be referred to as a Records Management Application (RMA) or Electronic Records Management System (ERMS).

   Applying basic records management concepts to electronic records will improve the management, accessibility, and use of information across the Department, as well as provide confidence for adequate and proper documentation of DOE's organization, functions, policies, decisions, procedures, and essential transactions.

3. AUTHENTICATION. Electronic records must be authenticated for the record's trustworthiness (i.e., the record is legible, complete, and an accurate representation of work performed). This process is accomplished by an individual or individuals who are competent to make that determination and certify or test to the validity, truthfulness, and accuracy of the record.

The authentication process is accomplished by manually affixing a seal, signature, initial, or an electronic representation thereof (such as a user ID/Password combination, biometric identification or digital signature), or other acceptable method of proof as to the genuineness, validity, and reliability of the record.

Public key cryptography, which is used to implement digital signatures, is one of the principal electronic signature technologies that agencies use when conducting business electronically. A Public Key Infrastructure (PKI) supports the application of digital signatures and is defined as "a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates". More information on PKI Digital Signature Authentication and Secured Transaction Action Records can be found at: http://www.archives.gov/records-mgmt/policy/pki.html.

4. SECURITY OF ELECTRONIC RECORDS. Electronic records must have controls in place to:

   a. Prevent unauthorized addition, modification, or deletion of a record

   b. Protect the records against power interruptions

   c. Provide an audit trail for addition, modification, or deletion of records, and retrieval activity

   d. Prevent over-writing of a record

   e. Prevent deletion of a records identifier once it is defined

   f. Prevent deletion of indexes, categories, labeling, or other 'pointers' of record identification

   g. Retain the record in usable format until its authorized disposition date

   h. Provids adequate recovery/rollback procedures and rebuild procedures so that records may be recovered or restored following s system or storage media malfunction

   i. Maintain the integrity of redacted records and assure that redacted material is not accessible.

5. SELECTION AND MAINTENANCE OF ELECTRONIC STORAGE MEDIA. Appropriate media for storing Department records throughout their life must meet the following requirements:

   a. Permit easy retrieval in a timely fashion

b. Facilitate distinction between record and nonrecord material

c. Retain the records in a usable format until their authorized disposition date

d. Make provisions for destruction moratoria when records have met their retention period to accommodate litigation and epidemiology freezes

e. If the media contains permanent records and does not meet the requirements for transferring permanent records as outlined in Chapter IX, permit the migration of the permanent records at the time of transfer to a medium which does meet the requirements.

f. Consider the following factors before selecting a storage medium or converting from one medium to another:

(1) The authorized life of the records, as determined during the scheduling process;

(2) The maintenance necessary to retain the records;

(3) The records density;

(4) The cost of storing and retrieving the records;

(5) The access time to retrieve stored records;

(6) The portability of the medium (that is, selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another (such as from optical disk to magnetic tape); and

(7) Whether the medium meets current applicable Federal Information Processing Standards.

g. Avoid the use of diskettes for the exclusive long-term storage of permanent or unscheduled records.

h. Ensure that only authorized users can identify and retrieve information stored on diskettes, removable disks, or tapes by establishing or adopting procedures for external labeling.

i. Ensure information is not lost because of changing technology or deterioration when converting storage media to provide compatibility with the Department's current hardware and software. Before conversion to a different medium, determine that the authorized disposition of the electronic records can be implemented after conversion.

j. Back up electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error. Duplicate copies of permanent or unscheduled records must be maintained in storage areas separate from the location of the records that have been copied.

k. Test magnetic computer tapes no more than six months prior to using them to store electronic records that are unscheduled or scheduled for permanent retention. This test should verify that the tape is free of permanent errors and in compliance with National Institute of Standards and Technology or industry standards.

l. Maintain storage and test areas for computer magnetic tapes containing permanent and unscheduled records at the following temperatures and relative humidity:

- Constant temperature – 62 to 68° F.
- Constant relative humidity – 35% to 45%

m. Read a statistical sample of all reels of magnetic computer tape containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss. In tape libraries with 1800 or fewer reels, a 20% sample or a sample size of 50 reels, whichever is lager, should be read. In tape libraries with more than 1800 reels, a sample of 384 reels should be read. Tapes with ten or more errors should be replaced and, when possible, lost data shall be restored. All other tapes which might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) shall be read and corrected as appropriate.

n. Copy permanent or unscheduled data on magnetic tapes before the tapes are ten years old onto tested and verified new tapes.

o. For magnetic tapes used to store permanent or unscheduled records, provide unique identification for each reel on external labels including the name of the organizational unit responsible for the data, system title, and security classification, if applicable. Additionally, the following information must be maintained for (but not necessarily attached to) each reel used to store permanent or unscheduled electronic records: file title(s); dates of creation; date of coverage; the recording density; type of internal labels; volume serial number, if applicable; number of tracks, character code/software dependency; information about block size; and reel sequence number, if the file is part of a multi-reel set. For numeric data files, include record format and logical record length, if applicable; data set name(s) and sequence, if applicable; and number of records for each data set.

p. Prohibit smoking and eating in magnetic computer tape storage libraries and test evaluation areas that contain permanent or unscheduled records.

q. Issue written procedures for the care and handling of direct access storage media which draw upon the recommendations of the manufacturers.

6. RETENTION AND DISPOSITION OF ELECTRONIC RECORDS.

a. Electronic records must be retained in a usable and easily retrievable format for the life of the record.

b. Electronic records may not be deleted or otherwise disposed of without prior disposition authority from NARA. See Chapter III for more detailed information on the disposition process.

c. Schedule disposition of electronic records, as well as related documentation and indexes, during the CPIC process, but no later than one year, after implementation of the system. [36 CFR 1234.32(a)]

d. Freedom of Information Act (FOIA). Electronic records can only be destroyed according to the time frame provided in an approved records disposition schedule. DOE is not legally bound to produce records under the Freedom of Information Act (FOIA) or legal discovery actions if the records have been destroyed according to the approved disposition schedule. However, this applies only if records destruction takes place on a regular basis as part of the normal course of business. This defense will not be available to offices with no demonstrable history of destroying records according to DOE schedules. More information on requirements and policy regarding FOIA can be found at NARA's website: http://www.archives.gov/foia/. **Note**: Regardless of the disposition requirements of a schedule, records destruction must be suspended if a FOIA or legal discovery action is pending or if there is a reasonable expectation of a FOIA or legal discovery action.

CHAPTER III. RETENTION AND DISPOSITION OF ELECTRONIC RECORDS

1. INTRODUCTION. A records disposition schedule places a value on the information contained within the records, the risk assessed in the event of loss, and is DOE's application of the laws and regulations governing records disposition in the Federal government. Concealment, removal, mutilation, obliteration, or destruction of records can subject employees to criminal penalties, including a fine, up to 3 years in Federal prison, and disqualification from government employment (18 U.S.C 2071). The Records Disposition Schedule is DOE's tool to avoid violating applicable laws and regulations, while permitting records to be handled according to their value and the risk assessed in the event of loss. Failure to follow instructions in the disposition schedule can result in legal consequences.

Currently, the DOE records disposition schedule is a traditional schedule that shows as separate items agency records series and systems, which are individually scheduled for appropriate disposition. In order to make the record schedules more useful to organizations implementing a records management application, DOE is developing flexible larger aggregates (i.e., big buckets) that will replace the disposition schedule now in use. These aggregates are being developed using DOE's lines of business identified in DOE's enterprise business model and will be cross-referenced to existing schedules

Figure 1 blow illustrates the flexible larger aggregates (i.e., DOE taxonomy) as it relates to the retention schedule. Figure 2 is a further breakdown for the Environmental Line of Business

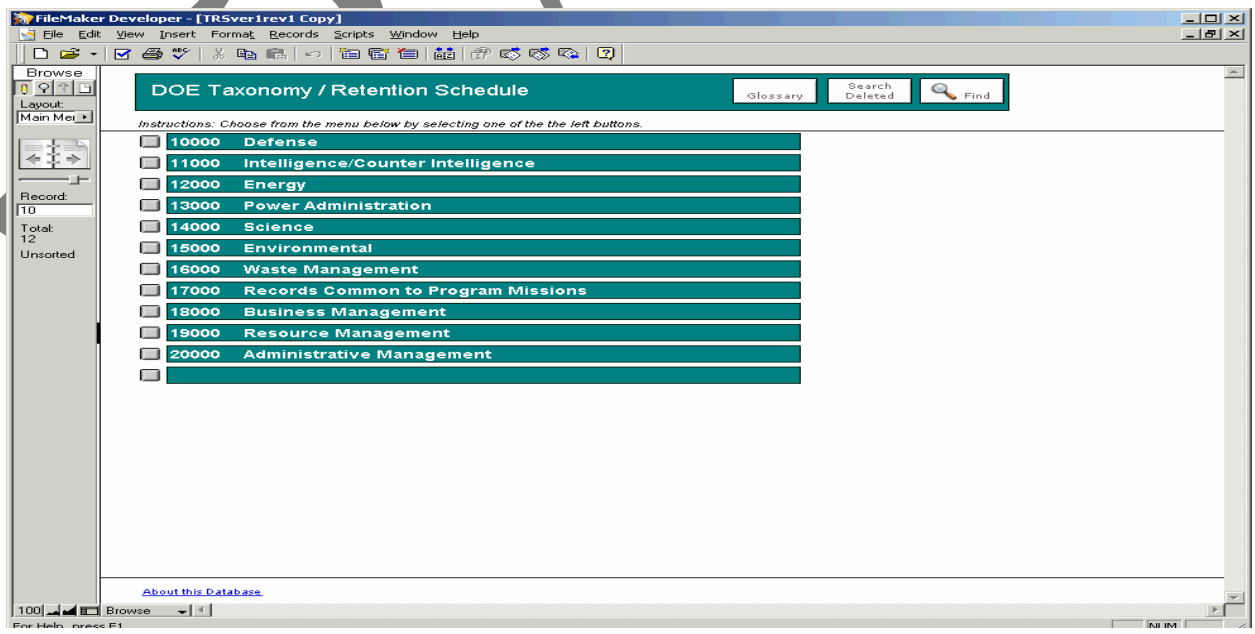

Figure 1. Illustration of DOE Taxonomy/Retention Schedule

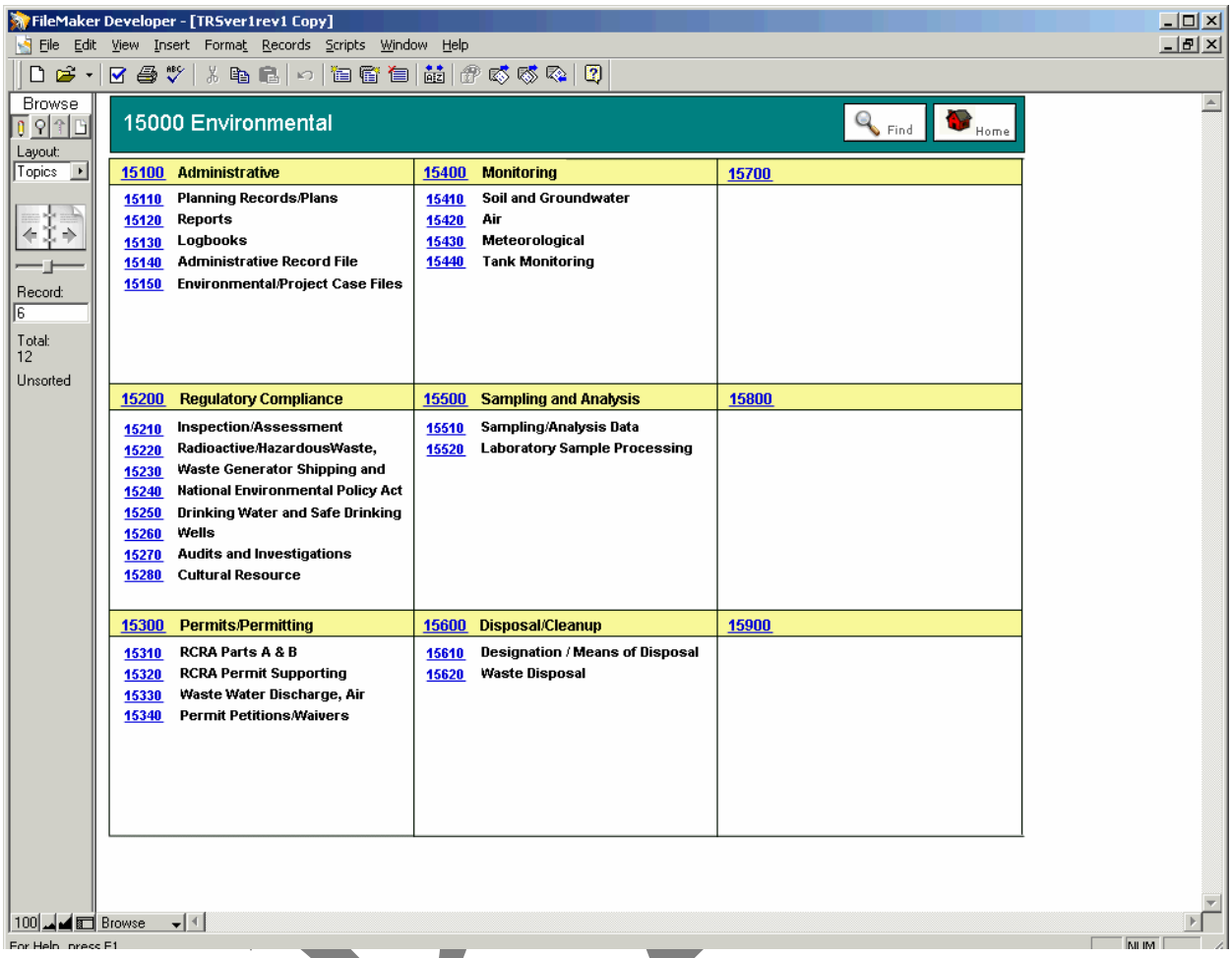

Figure 2. Retention Taxonomy for Environmental Records

2. ELECTRONIC RECORDS ARCHIVE (ERA). The ERA has been developed by NARA and is a comprehensive, systematic, and dynamic means for preserving virtually any kind of electronic record, free from dependence on any specific hardware or software. ERA will make it easy for National Archives customers to find records they want and easy for the National Archives to deliver those records in formats suited to customer's needs, Pre-accessioning permanent records into the ERA is a service that is offered that allows NARA to process electronic records early in the life cycle before potential loss of access and intellectual control due to technological and program change. An added benefit to the Department is that long-term preservation of the records is turned over to NARA.

3. RECORDS DISPOSITION. Records disposition refers to actions taken regarding records no longer needed to conduct regular, current business. Title 44 U.S.C. 2901(5) defines records disposition as any activity with respect to:

a. Disposal of temporary records no longer needed for the conduct of business by destruction or donation to an eligible person or organization outside of Federal custody in accordance with the requirements of 36 CFR 1228,

b. Transfer of records to Federal agency storage facilities or records centers,

c. Transfer to the National Archives of the United States (NARA) records determined to have sufficient historical or other value to warrant continued preservation, or

d. Transfer of records from one Federal agency to any other Federal agency in accordance with the requirements of 36 CFR 1228.

Disposition of documentary material identified as a Federal record can only be dispositioned according to the appropriate DOE records disposition schedule. This applies to records maintained in any electronic format or system, including e-mail, databases, information systems, word processing, spreadsheets, presentations, and web pages.

4. RECORDS DISPOSITION SCHEDULE

a. NARA regulations require records disposition schedules for all records created and maintained by the Department. The records disposition schedules are approved by the Archivist of the United States and provide **mandatory** instructions for the disposal of temporary records and the transfer of permanent records.

b. Temporary records are maintained for as long as there is a business need for the information. Record retentions can range from as short as two weeks to as long as 75 years (or longer). Temporary records are destroyed or deleted at the end of their retention.

c. Permanent records have long-term informational, legal, or historical value and are maintained indefinitely by NARA. These records are generally maintained in-house by the Department for extended periods, usually between 10 and 25 years, before they are transferred to NARA. Because of their volatile nature, electronic records are often transferred sooner so NARA can ensure their preservation. See Chapter IX for more detailed requirements for electronic records with a retention period of permanent.

d. Departmental records disposition schedules are available on the DOE web site at http://cio.doe.gov/RBManagement/Records/dissched.htm. The schedules are arranged in three main categories, administrative, programmatic, and site-specific. Contact your Program Records Official, Records Liaison Official, or Records Management Field Officer for assistance in locating the appropriate schedule for your electronic records.

e. Records disposition schedules are based on the content or function of the records rather than their format. For example, there is no specific schedule for record copies of word

processing files. The word processing file for a contract statement of work is covered by a procurement schedule, while a word processing file for a performance evaluation is covered by a personnel schedule.

f. DOE's flexible records disposition schedules are intended to be media-neutral. This means that a single retention will apply to a record, regardless of whether it is maintained in hard-copy, on a database, on the web, or on a share drive. When documentary materials exist in multiple formats, offices must determine which format constitutes the recordkeeping or "official" copy and apply the schedule retention to that copy. All other copies become reference materials that can be deleted when no longer needed.

5. SCHEDULING MAJOR ELECTRONIC INFORMATION SYSTEMS. Major electronic information systems (EISs) are required to have their own records disposition schedules. This applies to information systems supporting the five Departmental lines of business; Defense, Energy, Environment, Science, and General Management. EIS schedules provide separate dispositions for system components, including;

a. Data Inputs. Data used to populate an electronic information system must be managed according to the appropriate records disposition schedule. Data inputs can be electronic (e.g., ASCII files, delimited text files, image files, database tables) or hard-copy (e.g., forms and other text documents) and are generally disposable after the data has been verified in the master file or when it is no longer needed to support the reconstruction of the master file.

An EIS often shares data electronically with another EIS. In this instance, the data input has no physical form that requires disposition. The data on the sending system (data output) is covered by the retention schedule for that system. The data acquired by the receiving system (data input) is covered by the schedule for that system.

Consider the example of a timekeeping system that automatically transfers the number of hours an employee works each week to a personnel management system. The schedule for the timekeeping system may call for the hours-worked data to be kept for two weeks, while the schedule for the personnel management system may require the hours-worked data to be kept for 75 years.

b. Master File. The collection of data that provides the current informational content of the EIS. The information in the master file is used to support the business function of the EIS. The disposition of the data reflects the business needs of the Department and is defined in the records disposition schedule.

Some EIS master files are appraised by NARA as permanent records and must be transferred to NARA according to the time frame in the records disposition schedule.

Permanent EIS data records should be transferred to NARA when significant events occur in the EIS system development life cycle. These events include:

(1) Major version changes

(2) Conclusion of an update cycle

(3) Replacement by a new system

(4) Migration to another system

(5) System close-out or termination

Master files should be transferred to NARA in accordance with the requirements found in Title 36 Code of Federal Regulations (CFR) 1228, Subpart L [36 CFR 1228.270].

c. Data Outputs. Products generated from an EIS, including printouts, tables, charts, reports, screens of information, and electronic files used for other purposes. These records are disposed of according to the schedule covering the function for which they were produced. For example, if a contract management system is used to produce a report on yearly contracting costs for budgeting purposes, the disposition of the report would be covered by the schedule for budget planning, not the schedule for the contract management system.

d. System Documentation. Information on how the system captures, manipulates, and outputs data, including user manuals, administrator manuals, codebooks, data dictionaries, program source code listings, and other descriptive and technical materials. Documentation for temporary systems can be destroyed when superseded or obsolete, or when the system data is deleted. Documentation for permanent systems must be transferred to NARA when the master files are transferred.

e. System Software. Programs used to control the computer and develop and run application programs. System software should be deleted when superseded by routine software program updates and a quality assurance check is completed, or when no longer needed. This applies to system software for permanent records, as well as temporary records, because NARA requires system data to be transferred in software-independent formats.

Contact your Program Records Official, Records Liaison Official, or Records Management Field Officer for assistance in locating the appropriate schedule for your EIS.

CHAPTER IV. ELECTRONIC RECORDS MANAGEMENT

1. INTRODUCTION

Electronic records management (ERM) is using automated techniques to manage records regardless of format. Electronic records management is the broadest term that refers to electronically managing records on varied formats, be they electronic, paper, microform, image, etc. ERM is automation of records management processes and procedures. Electronic recordkeeping (ERK) is a subset ERM, because ERK focuses on electronically managing electronic records.

ERK is the development of automated processes an agency uses to manage its electronic records. These automated processes support not only the preservation of an electronic record's content, but also its context and structure over time.

An Electronic Recordkeeping System (ERKS) or Records Management Application (RMA) is an information system that is designed to meet the Department's recordkeeping needs. At a high level, NARA has defined an ERKS as an electronic information system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition. From a records perspective, an ERKS will ensure that the records it maintains will have sufficient authenticity and reliability to meet all of the Department's recordkeeping needs.

Not all of the requirements for managing records electronically will be implemented as automated "system functions". Some functional requirements may be implemented through non-automated organizational policies, practices, or records management procedures. For example, instead of a system-generated notice that specific records are eligible for destruction or transfer, an authorized user would need to query the system for those records based on predefined attributes.

2. INTEGRATION OF ELECTRONIC RECORDKEEPING. In some cases, electronic recordkeeping is used in conjunction with document management, content management, or records management applications in order to provide for the full set of capabilities. Electronic recordkeeping can be integrated with systems that create records in a number of ways:

a. Stand-alone – Electronic recordkeeping (ERK) does not directly interact with any other electronic-record-generating applications. RM or other staff (not the record's creator) files electronic records into the system. In this situation, the records are usually collected by a central organization who either (1) converts the record to an electronic medium (such as paper to a digital image), or migrates the record from its digital format to another digital format (e.g., Word format to PDF format) prior to inclusion into the recordkeeping system.

b. Integration with desktop software applications – ERK is integrated with various desktop applications (e.g., word processing, e-mail, and spreadsheet). This type of integration usually requires that the record creator actually declare the status of the record (e.g., record or nonrecord), categorize, and file the record. RM metadata is automatically received from the record-generating application.

c. Integration with an EDMS – Record-creating-end users interact with an electronic document management system (EDMS) in the foreground, while the EDMS interacts with an Electronic Recordkeeping System (EKRS), which is running in the background. Using this option requires that the EDMS have a defined process, flag, or business rule that transfers the record into the ERKS at its completion.

d. Total integration within EIS design – Electronic recordkeeping functionality is integrated into the requirements definition of Departmental, mission-supporting, electronic information system (EIS) design when that EIS contains data qualifying as a Federal record.

3. GENERAL REQUIREMENTS. Not all of these requirements will necessarily be implemented as automated "system functions" in electronic records management or an electronic recordkeeping system. Some functional requirements may be implemented through non-automated organizational policies, practices, or records management procedures. Therefore, for the purpose of this section, the broader term of Electronic Records Management (ERM) Electronic records management is used. ERM must provide for:

a. Assigning Unique Identifiers. Unique identifiers must be assigned to records and their associated metadata.

b. Capturing Records. ERM should allow import of records from other sources. This may involve format conversion for records that are imported from external information systems (in which case records are physically captured and transported to the recordkeeping system). Or, ERM should also establish a link from the electronic record to a record in an external system in order to establish records management control (in which case physical transport of the records from one system to another isn't required).

c. Implementing a File Plan. A File Plan is a defined and controlled hierarchical folder structure that relates categories of records (i.e., contents of the folders) to a NARA-approved records retention schedule. Only authorized individuals are permitted to create, add, edit, or delete the folder structure.

d. Identifying and Filing Records. Users must be able to select and place records in the appropriate file folder. Once a unique computer-generated record identifier is assigned to a record, the contents of the record are locked down and no modifications can be

made to that record. In the event a modification is needed to the record, the record must be resubmitted as a new version of the record. Metadata about the record must be captured at the time the record is filed.

e. Filing Electronic Mail Messages. E-mail messages, including attachments, must be filed in the same manner as other electronic records.

f. Storing Records. ERM must provide or interface with a repository for storing electronic records that meets the security requirements in Chapter 2, section 4.

g. Scheduling Records. ERM must provide the capability to automatically track the disposition schedules of records and handle three types of disposition instructions:

(1) Time dispositions where records are eligible for disposition immediately after completion of a fixed period of time.

(2) Event disposition where records are eligible for disposition immediately after a specified event takes place.

(3) Time-event dispositions where the retention periods of records are triggered after a specified event takes place.

h. Screening Records. ERM provides for viewing, saving, and printing list(s) of records within folders based on a variety of qualifiers (e.g., by user, organization, disposition instruction codes, etc.)

i. Retrieving Records. Flexible searches must be allowed that will accommodate defined criteria. Additionally, access control must be in place to ensure only authorized personnel are allowed to view records.

j. Transferring Records. Using disposition instructions, ERM must identify and present those records eligible for transfer.

k. Destroying Records. Using NARA-approved disposition schedules, identify and present those records that are eligible for destruction. Once approved for destruction, ERM must delete the record and/or metadata stored in the repository in a manner such that the record cannot be physically reconstructed. However, ERM must also provide for destruction moratoria when records have met their retention period to accommodate litigation and epidemiology freezes.

l. Access Control. ERM must provide capability to define groups of users and access criteria.

m. System Audits. ERM must provide an account of records capture, retrieval and preservation activities to assure the reliability and authenticity of a record. Audit utilities must provide a record of transfer and destruction activities. Only authorized individuals shall be allowed to enable/disable the audit functions and to backup and remove audit files from the system.

n. System Management Requirements. Backup capability is typically provided by the operating system or a Datebase Management System (DBMS). ERM must provide the capability to automatically create backup or redundant copies of the records, as well as their metadata. The method used to backup electronic records shall provide copies of the data that can be stored off-line and at separate location(s) to safeguard against loss of records, metadata, and other records management information due to system failure, operator errors, disaster, or willful destructions. Recovery/rollback and rebuild capabilities for the electronic records must be maintained. Storage space must be monitored and appropriate actions taken to ensure adequate storage availability.

o. Accessibility. Electronic records must be available on a shared drive or server that is accessible to users with a need for the information.

4. CREATION AND USE OF TEXT DOCUMENTS. An electronic record that is maintained in its original format as the official record copy must meet the following minimum requirements:

a. Provide a method for all authorized users of the system to retrieve desired documents, such as an indexing or text search system;

b. Provide an appropriate level of security to ensure integrity of the documents;

c. Provide a standard interchange format when necessary to permit the exchange of documents on electronic media between Department computers using different software/operating systems and the conversion or migration of documents on electronic media from one system to another; and

d. Provide for the disposition of the documents including, when necessary, the requirements for transferring permanent records to NARA. See Chapter IX of this document for additional information on permanent electronic records.

5. ELECTRONIC RECORDKEEPING SYSTEMS (ERKS). An ERKS may also be referred to as an Electronic Records Management System (ERMS) or a Records Management Application (RMA) and is an electronic information system that has been designed to collect, organize, and categorize its records/data to facilitate their preservation, retrieval, use, and disposition.

a. ERKS Software. Software used as a records management application for electronic recordkeeping must conform to DOE STD-4001-2000, Design Criteria Standards for Electronic Records Management Software Applications (http://www.eh.doe.gov/techstds/standard/std4001/std400100.pdf. This standard is based on DoD 5015.2-STD, Department of Defense Electronic Records Management Software Application Design Criteria. There are a number of software products that have been certified as meeting the functional requirements of DoD 5015.2 (see http://jitc.fhu.disa.mil/recmgt/register.html). In the event the selected software has not been DoD 5015.2 certified, the software must be certified against DOE STD-4001-2000.

b. ERKS Functions. The primary management functions of an ERKS are to:

(1) Categorize and locate records,

(2) Identify records that are due for disposition,

(3) Automate all the processes identified in sections 3 and 4 above.

Examples of where use of a certified ERKS can facilitate records management include managing records for desktop applications where the electronic version of the record will be the recordkeeping copy; maintaining electronic mail in an electronic form for recordkeeping purposes; and facilitating the transfer of permanent electronic records to the National Archives and Records Administration.

CHAPTER V. ELECTRONIC INFORMATION SYSTEMS

1. INTRODUCTION. An electronic information system (EIS) is the collection of technical and human resources that provide the storage, computing, distribution, and communication for the information required by all or some part of the Department. An EIS automates programmatic and administrative business functions and produces Federal records in the process.

2. RECORDS MANAGEMENT AND ELECTRONIC INFORMATION SYSTEMS

   a. System developers are responsible for:

      (1) Ensuring incorporation of records management and archival functions into the design, development and implementation of the information system by including the appropriate Program Records Official, Field Records Officer, and/or Records Liaison Officer in all phases of the system development lifecycle.

      (2) Developing and maintaining up-to-date documentation about electronic information systems that is adequate to:

         (a) Specify all technical characteristics necessary for reading or processing the records;

         (b) Identify all defined inputs and outputs of the system;

         (c) Define the contents of the files and records;

         (d) Determine restrictions on access and use;

         (e) Understand the purpose(s) and function(s) of the system;

         (f) Describe update cycles or conditions and rules for adding information to the system, changing information in it, or deleting information; and

         (g) Ensuring the timely, authorized disposition of the record.

      (3) Including the appropriate Program Records Official, Records Liaison Officer, or Field Records Officer in all phases of the systems development lifecycle.

      (4) Ensuring systems are not rolled over, decommissioned, or migrated without the concurrence of the Program Records Official, Field Records Officer, or Departmental Records Officer.

   b. The office with ownership of the system is responsible for:

(1) Ensuring the value of the system and its data has been evaluated and is reflected in a NARA-approved records disposition schedule.

(2) Coordinating the disposition of the system and its data with the appropriate Program Records Official, Records Management Field Officer, or Records Liaison Officer.

(3) Ensuring a process and procedures are in place to follow the disposition instructions in the NARA-approved records disposition schedule.

c. The Program Records Officer is responsible for reviewing each proposed EIS to determine:

(1) Application of a NARA-approved records disposition schedule has been properly applied to the system, or the process has been initiated to develop a new schedule.

(2) Processes and procedures are place to ensure the dispositions can be carried out.

3. DISPOSTION OF SYSTEM INFORMATION AND DATA. Before a system can be retired, rolled over, or decommissioned, the Program Records Official must be contacted to verify the system and its data has been scheduled for disposition, and that the retention period has been satisfied. The data and system documentation must be maintained accessible until the expiration of the approved retention period.

4. SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC). It is important to note that the records life cycle is distinct from the systems life cycle. The systems life cycle or systems development life cycle (SDLC) applies to agency processes for developing and implementing agency information systems. The records life cycle, on the other hand, demands that agencies manage their records from creation through final disposition regardless of the system in which they reside. The most effective way to manage electronic records is to embed records management requirements into each stage of the SDLC.

The following are SDLC records management objectives and related questions for project managers and teams to consider at each phase of the SDLC.

a. Concept Development: The records management objective of concept development is to get records staff involved in the initial system design so records issues can be identified and discussion can begin on records disposition schedules.

(1) Is this system replacing a paper-based system? If yes, are the paper records already scheduled? If yes, can the existing dispositions be used as the basis for new dispositions for the system?

(2) Is this new system replacing an existing electronic system? If yes, are the existing electronic records already scheduled? If yes, can the existing dispositions be used as the basis for new dispositions for the system? Has migration of legacy data been addressed?

(3) If the business process/workflow in question has been or will be redesigned prior to system development, will the new business process account for a change in the nature of the existing records?

(4) Has the records officer signed off as a stakeholder on the IT Investment Proposal summary?

b. Requirements Definition: The records management objectives in this phase ensure that all records-related requirements have been identified and formally documented in the system requirements document. To be implemented effectively, the records management requirements should be validated and measurable.

(1) Have all records management requirements been incorporated into the system?

(2) Are there any additional requirements based on business needs?

(3) How will the proposed records dispositions and retention times impact the records-related requirements? Is there a documented migration strategy that will ensure the integrity and continued access to records of long-term value?

(4) Are all the records-related requirements detailed in the system requirements documentation incorporated into the records requirement section of your draft IT investment proposal?

(5) Have the requirements been validated and have clear measures been developed for each?

c. Preliminary and Detailed Design: The records management objectives in this phase ensure that the requirements identified in the previous phases are addressed in the preliminary and detailed system design, and to initiate the draft records schedule.

(1) Are all identified records management requirements integrated into the system design?

(2) Has the draft records schedule for the system been finalized and circulated for internal clearances?

(3) Has the records staff reviewed the draft schedule to ensure all the identified records-related requirements are covered?

(4) Have existing records management service components been identified and incorporated into the system design? Service components are available at: https://collab.core.gov/CommunityBrowser.aspx?id=1.

(5) Has the records officer signed off as a stakeholder on the requirements of the Preliminary Design Document?

(6) Has the records officer been included in project status meetings?

d. Integration and System Test: The records management objective in this phase is to validate the system meets the specific records management requirements identified in the requirements definition stage, and that the system is scheduled.

(1) Has the Departmental Records Officer submitted the records schedule to NARA?

(2) Does the system meet all the identified records-related requirements outlined in the requirements document? If not, consult with the records staff to determine the appropriate course of action.

(3) Has the Configuration Control Board (CCB) process taken records management issues into account for all changes?

(4) Has the records officer signed off as a stakeholder on the Systems Test Report?

e. Production and Operation: The records management objectives in this phase are to either validate the records schedule or modify it to reflect the findings of the assessment, and re-certify that records management requirements are being met throughout the system's Operations and Maintenance (O&M) phase.

(1) Are the records management requirements being followed?

(2) Has the system been modified or is it being used to support different business needs than originally planned? If so, a new product plan or schedule may be required.

(3) Is the system consistent with what was intended? For example, is the system maintaining more, less, or different data than intended? If yes, the records schedule may need to be modified.

(4) Are the records management issues reviewed with the records officer on a regular basis?

(5) Has the records officer signed off on project review certification documents?

f. System Retirement and Rollover: The records management objectives in this phase are to ensure continued accountability for the records contained in the system being shut down, and to ensure records are retained and kept accessible for the full retention period.

(1) Is the system being totally shut down or will some data migrate to a successor system?

(2) If data is to be migrated, will the functionality of the migrated data be preserved and will access be provided to the data that is not migrated?

(3) If the system is being totally shut down, will the data be accessible for the full retention period provided by the schedule?

(4) Is the current disposition of the system still appropriate? Have business needs sufficiently changed to warrant a re-examination of both the value of the records and the retention period?

(5) Has the records officer signed off on the shut-down documentation certifying all records management concerns have been addressed?

5. INFORMATION TECHNOLOGY CAPITAL PLANNING AND INVESTMENT CONTROL (CPIC).

a. GENERAL. OMB Circular No. A-130, Management of Information Resources, establishes policy for the management of Federal information resources. This circular requires agencies to establish and maintain a Capital Planning and Investment Control (CPIC) process that links mission needs, information, and information technology in an effective and efficient manner. Agencies' CPIC process is required to build an Enterprise Architecture (EA) and transition to the target architecture of the Federal government.

The DOE CPIC process encompasses the submission of all major IT investment information to the OCIO for evaluation and resultant recommendation to the Corporate Review Board for inclusion, or continued inclusion, in the Department IT investment portfolio and budget submissions. OMB and the Department have defined major IT investments, including large infrastructure investments, as those that meet any of the following criteria:

(1) Total project cost of $5 million or more (i.e., cumulative Development/Modernization/Enhancement (D/M/E) funding across all fiscal years (all past, current, and all future) of the project

(2) Any investment with cumulative steady state or mixed lifecycle funding of $5 million or more across the Prior Year, the Current Year, and the Budget Year

(3) A financial system with an estimated investment cost of $500K or more in one year

(4) An interagency e-Government initiative or line of business where DOE is the lead agency **and** existing major IT investments targeted for migration to an e-Government line of business in FY 2006 or FY 2007

(5) OMB directed portfolio IT investments (e.g., infrastructure and enterprise architecture)

(6) Requires special management attention because of its importance to the agency mission

(7) Has high development, operating, or maintenance costs, high risk or high return

(8) Plays a significant role in the administration of agency programs, finances, property, or other resources

(9) A grants management IT investment, regardless of dollar value.

b. FEDERAL ENTERPRISE ARCHITECTURE (FEA). As part of the initiative to transform the Federal government to one that is citizen-centered and results-oriented, the Office of Management and Budget (OMB) has developed a Federal Enterprise Architecture (FEA). The FEA is being constructed through a collection of interrelated "reference models" designed to facilitate cross-agency analysis and the identification of duplicative investments, gaps, and opportunities for collaboration within and across Federal agencies. These models are defined as:

(1) Performance Reference Model (PRM)

(2) Business Reference Model (BRM)

(3) Service Component Reference Model (SRM)

(4) Data and Information Reference Model (DRM)

(5) Technical Reference Model (TRM)

c. FEA RECORDS MANAGEMENT PROFILE. The National Archives and Records Administration (NARA), in partnership with the OMB, has developed an FEA Records Management Profile to provide guidance on the application of records management resources to enterprise-wide organizations. The FEA RM Profile can be used

to (1) ensure that common and consistent records management procedures and practices are built into agency work processes, enterprise architectures, information systems, and CPIC processes, and (2) provide the framework for embedding common and consistent Records Management procedures and practices into agency business.

RM Resources	The FEA
OMB, ISO, NARA Guidance, DOE Disposition Schedules	Business Reference Model (BRM) Agencies analyze their business processes to help identify the records they create, receive, maintain and use.
RM Service Components (RMSC)	Service Component Reference Model (SRM) Agency use of records management service components will help automate the records management life cycle.
DoD 5015.2-STD NARA GPEA Guidance NARA Transfer Instructions	Technical Reference Model (TRM) Agency use of the TRM will help identify the standards, specifications, and technologies needed to support RMSC.
DoD 5015.2 Metadata Profile	Data Reference Model (DRM) Facilitate the transfer of records between RMSC and applications. Enable discovery and access by agencies and the public.
Industry Advisory Council (IAC) White Paper	Performance Reference Model (PRM) Agencies identify metrics and goals for records management performance and outcomes.

Figure 3. Viewing Records Management Through the FEA

d. DOE ENTERPRISE BUSINESS MODEL (EBM). In support of the FEA effort, DOE has developed an Enterprise Business Model (EBM) which follows its five Lines of Business (LOB): 1) Defense, 2) Energy, 3) Science, 4) Environment, and 5) General Management. The last, General Management LOB, cuts across the other four DOE Mission-related LOB's. The General Management LOB is further broken down into 15 functions, one of which, Information and Technology Management, includes Records Management as one of its sub-functions. Records Management cuts across all five of DOE's LOB's. This realignment will allow DOE to more effectively support e-Government initiatives, as well as minimize duplication of efforts. .

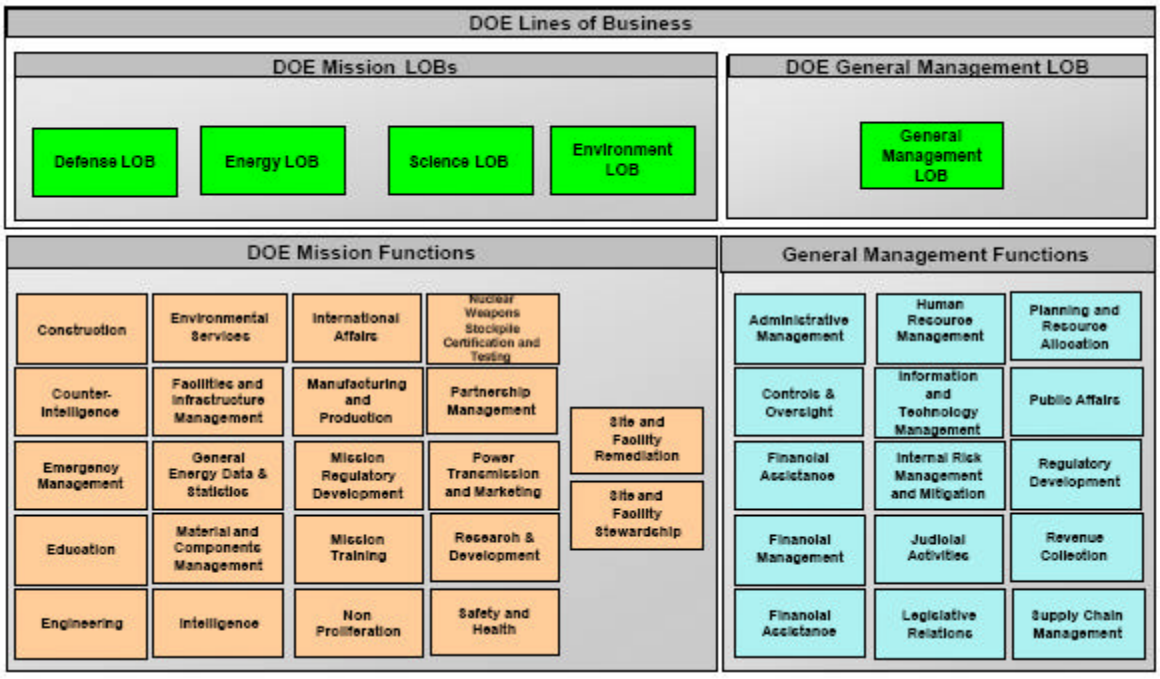

Figure 4. DOE Enterprise Business Model

6. USEFUL RESOURCES. There are a number of useful resources for evaluating ERM requirements in relation to CPIC and/or the FEA project:

   a. Determining how NARA's Records Management Profile fits within the FEA: (http://www.archives.gov/records-mgmt/policy/rm-profile.html).

   b. Evaluating CPIC programs in terms of ERM requirements: http://www.archives.gov/records-mgmt/policy/cpic-guidance.html)

   c. Aligning DOE programs to the ERM E-Government Initiatives implementation plan: (http://www.archives.gov/records-mgmt/policy/governance-guidance.html).

CHAPTER VI. ELECTRONIC MAIL RECORDS

1. INTRODUCTION.

Electronic Mail (e-mail) systems provide an excellent example of the dichotomy between the benefits of electronic records versus the burden associated with poor electronic records management practices. Through technological innovation, an application originally designed as a simple, electronic means of text communication between computer users on closed internal networks evolved into a globally-connected tool essential to Federal and commercial business. Today, with the exception of large Departmental information systems, most electronic records (e.g., documents, spreadsheets, presentations, etc,) are captured by, transmitted through, and stored in the e-mail system. However, that value can't be fully realized in support of the mission unless the information is organized for efficient access and retrieval by staff. Most user e-mail folders aren't available to others and they are rarely organized so that others can easily locate or access required information.

2. CAPTURE OF E-MAIL AS A RECORD

a. By 2009, DOE organizations must implement an electronic records management system to electronically capture e-mail. In the interim, record copies of e-mails with a retention period of 180 days or longer must be printed and retained in a recordkeeping system until the retention period has expired.

b. The individual transmitting or receiving electronic mail (e-mail) determines if the message is a record according to the definition in this manual.

c. E-mail records must be maintained appropriately to ensure the creation and maintenance of adequate and proper documentation of policies, programs and actions.

d. The individual transmitting or receiving an e-mail is responsible for filing the message in the organizational recordkeeping system. If the message provides documentation of a team project, or other collaborative effort that is copied to multiple addressees, the team will assign responsibility for filing the record copy to a specific individual.

3. MAINTENANCE AND USE OF E-MAILS

a. E-mail systems must provide users with the capability to organize their messages in folder-based structures and to maintain or "archive" messages on personal network drives or local hard drives. Because they are not available to others with the potential need to access the records, these personal e-mail folders may not be used to maintain records for their full life cycle, unless the record has a retention period of 180 days or

less. Upon determination that an e-mail message is a DOE record **and** has a retention lifecycle of more than 180 days, it must be moved to the organization's recordkeeping system.

b. As with paper correspondence, e-mail messages must be managed using best records management practices. In the case of e-mail, this includes using as full and complete a description as practical in the message subject line (for example, avoid writing in the subject line "minutes" or "important" or "report" which are too general to be of future reference or archival assistance).

c. E-mail messages and their corresponding attachments must be filed together in the recordkeeping system. If this is not possible, the message and its attachments must be cross-referenced in a paper recordkeeping system or linked in electronic recordkeeping systems.

d. To meet Federal regulations, enhance retrieval, and ensure the records can be understood in their proper context, the following metadata must be captured for each e-mail record, including those that may be retained in a hard copy recordkeeping system:

(1) Name and e-mail address of the sender

(2) Name and e-mail address of the addressee(s)

(3) If the addressee is a distribution list, include the names of all the members of the list

(4) Name and address of other recipient(s)

(5) Date and time the message was sent

(6) Subject of the message

(7) Date and time the message was received, if the e-mail system offers this capability

e. E-mail systems with calendars and/or task lists meeting the definition of a Federal record are to be managed in accordance to DOE Administrative Schedule 23, item 5, Schedule of Daily Activities.

4. <u>DISPOSITION OF E-MAIL RECORDS.</u>

a. E-mails of short-term (180 days or less) interest, with minimal or no documentary or evidential value, may remain in the user's personal e-mail folders until they are purged using the auto-delete feature of the e-mail system. If the system auto-delete feature is

not activated, users must manually delete the records when they are no longer needed. See DOE Administrative Schedule 23, item 7, Transitory Files, for examples of common records of this type. In order to avoid the accumulation of large volumes of data with minimal value, it is strongly recommended that the auto-delete feature of the e-mail system be used. Electronic records that are kept too long can create liabilities in regard to litigation discovery, FOIA, and the Privacy Act.

b. E-mails with a NARA approved retention period of longer than 180 days must be moved to the organization's recordkeeping system upon completion of the record.

c. Certain types of DOE records have been determined by NARA to have sufficient historical or other value to warrant continued preservation by the Federal government. Records Disposition Schedules provide information on which DOE records are permanent.

(1) E-mail messages covered by a permanent Records Disposition Schedule must be maintained in a manner that allows for the eventual transfer of the records to NARA.

(2) Permanent e-mail messages maintained in an electronic recordkeeping system must be transferred to NARA according to the instructions found in "Expanding Acceptable Transfer Requirements: Transfer Instructions for Existing E-mail Messages with Attachments."

d. E-mail messages that relate to an individual's own affairs such as professional organization meetings and that do not contain any information documenting DOE actions or activities are non-records that must be deleted as soon as they are no longer needed.

CHAPTER VII. WEB RECORDS

1. INTRODUCTION. There are two categories of web records that must be managed according to DOE and the National Archives and Records Administration (NARA) policies and regulations

   a. Web Content Records. Information presented on DOE Internet, intranets, virtual private networks, portals, and classified web sites, including:

      (1) The content pages that compose the site, inclusive of the HTML markup.

      (2) Records generated when a user interacts with a site.

      (3) Lists of the URLs referenced by the site hyperlinks, if the office chooses to document the site this way.

   b. Web Management and Operations Records. Materials documenting the development and maintenance of the web site, including:

      (1) Web site design records.

      (2) Records that specify DOE web policies and procedures, addressing such matters as how records are selected for the site and when and how they may be removed.

      (3) Records documenting the use of copyrighted material on a site.

      (4) Records relating to the software applications used to operate the site.

      (5) Records that document user access and when pages are placed on the site, updated, and/or removed.

      (6) Records that provide structure related to the site that include:

         (a) Site maps that show the directory structure into which content pages are organized, and

         (b) COTS software configuration files used to operate the site and establish its look and feel, including server environment configuration specifications.

2. CREATION AND RECEIPT.

a. Determining Record Status.

(1) It is the responsibility of the web content owner to determine if documentary materials posted on a DOE web site are records.

(2) It is the responsibility of the webmasters to determine if web content management and operational materials are records.

(3) The source code associated with the DOE facility Web Pages is a record that must be maintained in accordance with NARA-approved Records Disposition Schedule.

(4) To help determine which web sites contain records, it is necessary to determine how information is used. Generally, web sites are records if they:

(a) Provide information or customized information

(b) Collect data from the public or DOE staff or contractors

(c) Provide the public with access to information contained in databases

(d) Provide the public with the ability to electronically complete and file a DOE form

(e) Provide the public with an opportunity to electronically comment on DOE activities

3. MAINTENANCE AND USE.

a. Responsibility for Maintaining Records. The web content owner and the webmasters must coordinate their efforts to ensure that the content, context and structure of the web records are maintained.

(1) Content is the HTML-encoded page, additional content file reference in the page or content created by end users interacting with the web site or portal.

(2) Context refers to the administrative and technical records necessary for or produced as part of the management of the web sites.

(3) Structure is a site map indicating the arrangement of the web site's content pages and its software configuration files.

b. Due to the large volume and complexity of web records, NARA recommends the application of risk management concepts to the ongoing maintenance of web records. In this model, high risk web sites receive a commensurately higher level of records management effort than low risk web sites. NARA provides extensive instructions on conducting risk management evaluations of web records in the January 2005 edition of "NARA Guidance on Managing Web Records." http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html

4. DISPOSITION

a. The web content owner is responsible for ensuring that web content records are disposed of according to the appropriate schedule.

b. The webmasters are responsible for ensuring that web management and operations records are disposed of according to the appropriate schedule.

c. Applying Schedules.

(1) Web records must be captured and retained for the length of time required by the DOE Records Disposition Schedules. The appropriate schedule for a web record is determined by its subject matter and content, not the media in which it was distributed.

(2) DOE employees and contractors who are uncertain about which schedule covers a particular web record should contact their RLO.

d. Permanent Records. Certain types of DOE records have been determined by NARA to have sufficient historical or other value to warrant continued preservation by the Federal government. Records Disposition Schedules provide information on which DOE records are permanent.

(1) Web content records covered by a permanent records disposition schedule must be maintained in a manner that allows for the eventual transfer of the records to NARA. The hypertext functionality of the records must also be maintained (see Chapter 3, Section 3.5 of the NARA guidance document referenced in Section 3.b above for details).

(2) Permanent web records must be transferred to NARA according to the instructions found in "Expanding Acceptable Transfer Requirements: Transfer Instructions for Permanent Electronic Records Web Content Records." See Chapter III, Permanent Electronic Records Requirements, of this manual for a summary of transfer requirements for web records.

CHAPTER VIII. VITAL RECORDS

1. INTRODUCTION.

Vital records are those emergency operating records and legal and financial rights records required during and after an emergency or as part of the recovery from disaster.

a. Examples of emergency operating records include emergency plans and directives, orders of succession, delegations of authority, staffing assignments, selected program records, and related policy and procedural records.

b. Examples of legal and financial rights records include accounts receivable records, social security records, payroll records, retirement records, and insurance records.

c. Vital records may also include Electronic Information Systems (EIS) or portions of an EIS needed to carry out operations and ensure legal and financial rights during and after an emergency.

d. Consult 36 CFR 1236: Management of Vital Records http://www.archives.gov/about/regulations/part-1236.html for further information.

2. VITAL RECORDS PROGRAM. Each DOE element must develop and implement a vital records program that includes:

a. Procedures for identifying, protecting, controlling access to, and ensuring availability of records and information systems that:

(1) Specify how the organization will operate in case of an emergency and how it will support civil defense associated with disasters and attacks;

(2) Are needed for the continued operations and missions delivery of the organization both during and after an emergency or disaster; and

(3) Are essential to the preservation of the legal rights and interests of the Government and its citizens.

b. Procedures for accessing records required to support critical activities the organization performs when operating under abnormal business conditions and/or in a location other than the normal place of business.

c. Plans or procedures for establishing and maintaining a vital records inventory that identifies:

(1) Requirements for proper labeling and handling of vital records,

(2) Security precautions,

(3) Frequency of updates,

(4) Media, hardware, software, and supporting service needs; and

(5) Provisions for access from remote locations.

d. An inventory system that identifies hard copy and electronic records by:

(1) Series or system title,

(2) Description,

(3) Type,

(4) Name of office and individual responsible,

(5) Physical location of records, and

(6) Date of latest update

e. Provisions to ensure protection against and assessment of records damage or loss.

f. Provisions for the timely and efficient assessment of records damage or loss and for recovering records affected by an emergency or disaster.

g. Provisions for storing and maintaining records that includes:

(1) Duplicate copies of the vital records and associated inventory must be maintained at separate locations to ensure immediate access in any situation.

(2) Records must be maintained in a medium that is most viable for readability and under post-attack conditions, including the appropriate hardware and software necessary to access the records.

(3) Electronic records must be evaluated and stored as necessary regarding volume; frequency of update; electricity, computers, and software support services available to support records access and use; and accessibility from remote locations via virtual private networks or compact disks.

(4) Storage/backup protection methods must be selected based on evaluation of the effectiveness of the protection; cost; degree of risk for potential loss; physical susceptibility to destruction; and need for special environmental conditions for transport, storage, and update.

(5) Ability to retrieve records quickly during an emergency or disaster

h. It is imperative that vital records be reappraised continually and reviewed at least annually to ensure that changing conditions are addressed and that records are up-to-date and immediately accessible.

i. A plan must be developed and maintained to recover records that are damaged in an emergency disaster, regardless of media. This plan must include the priorities for restoring or recovering multiple damaged systems and the options for recovery and replacement. This plan must also include a resource list of local disaster recovery firms that can easily assist in restoration and employment contact lists and vital records inventories, which must be maintained at multiple off-site locations to facilitate their use.

j. NARA's "Vital Records and Records Disaster Mitigation and Recovery: An Instructional Guide" can be found at http://www.archives.gov/records-mgmt/vital-records

3. STORAGE CONSIDERATIONS

a. Locations. Locations where vital records will be stored, such as alternate emergency operations centers (EOCs), command centers, and relocation sites must provide adequate protection and accessibility and meet the improved risk level fire protection required by DOE O 420.1B, Facility Safety, dated 12-22-05. Before classified documents can be stored at these locations, approval must be granted in accordance with DOE O 470.4, Safeguards and Security Program, dated 8-26-2005.

b. Manner of Storage. Records will be stored to ensure ease of access, retrieval, and control. Storage systems will allow for timely access. Classified and unclassified records must be handled in accordance with DOE O 471.1A, Identification and Protection of Unclassified Controlled Nuclear Information, dated 6-30-00, and DOE O 471.3, Identifying and Protecting Official Use Only Information, dated 4-9-03-2005.

4. DISPOSITION OF VITAL RECORDS. The official record copy of vital records must be maintained for the period of time specified in the DOE records disposition schedules. Duplicate copies of vital records stored in the separate locations should be deleted when obsolete or superseded and replaced with an updated revision.

5. REFERENCES. Additional information on emergency operations records can be found at:

a. DOE O 151.1B, *Comprehensive Emergency Management System*, dated 10-29-03 (directives online at www.directives.doe.gov).

b. DOE N 150.1, *Continuity of Operations*, dated 1-14-05.

c. DOE G 151.1, *Emergency Management Guide*, dated 8-21-97.

DOE O 243.2, *Vital Records*, dated 2-2-06

e. DOE O 420.1A, *Facility Safety*, dated 5-20-02.

f. 36 CFR 1236, which prescribes policies and procedures for establishing a program for the identification and protection of vital records needed for continuity of Agency operations before, during, and after emergencies and needed to protect the legal and financial rights of the Government and persons affected by Government activities (www.gpoaccess.gov/index.html).

CHAPTER IX. PERMANENT ELECTRONIC RECORDS

1. INTRODUCTION. Permanent records are DOE documentary materials that are determined by the National Archives and Records Administration (NARA) to have sufficient historical or other value to warrant their continued preservation by the Government. Such records document the Department's origins, organization, functions, significant transactions, and activities with significant research or reference value.

   DOE permanent records must comply with the objectives of NARA's Electronic Records Archives (ERA) which is a comprehensive, systematic, and dynamic means for preserving virtually any kind of electronic record, free from dependence on any specific hardware or software. ERA will make it easy for NARA customers to find records they want and easy for the NARA to deliver those records in formats suited to customer's needs. . More information on the ERA can be found at http://www.archives.gov/era.

   With a few exceptions, permanent Federal records are transferred to the custody of NARA. NARA takes ownership of the records and becomes responsible for their archival preservation and for making the records available to the public, as appropriate.

   Examples of permanent DOE records include:

   - Directives
   - Mission-related publications
   - Level I Research and Development Records
   - Radioactive waste disposal records
   - EIA (Energy Information Administration) survey processing records

2. CHARACTERISTICS OF PERMANENT ELECTRONIC RECORDS. Permanent records generally:

   a. Retain their importance for documenting legal status, rights and obligations of individuals, groups, organizations, and governmental bodies despite the passage of time;

   b. Provide evidence of significant policy formulation and business processes of DOE;

   c. Provide evidence of DOE's conduct of foreign relations and national defense;

   d. Provide evidence of DOE organization, deliberations, decisions, and actions relating to major social, economic, energy, and environmental issues;

e. Provide evidence of the significant effects of DOE programs and actions on individuals, communities, and the natural and man-made environment;

f. Contribute substantially to knowledge and understanding of the people and communities of our nation.

3. SELECTION AND MAINTENANCE OF STORAGE MEDIA. Permanent electronic records managed by DOE offices must be stored and maintained on media meeting the requirements found in Title 36 Code of Federal Regulations (CFR) 1228, Subpart C [36 CFR 1234.30]. This regulation provides guidance on:

a. Selecting appropriate media and systems for maintaining electronic records.

b. Ensuring that electronic records are not lost and that the authorized dispositions can be implemented after conversion to a new storage medium or system.

c. Standards for maintaining magnetic computer tapes and direct access storage media.

d. Ensuring that electronic storage media and systems are capable of retaining the records in a usable format until their authorized disposition date.

4. PRE-ACCESSIONING ELECTRONIC RECORDS. Pre-accessioning takes place when an organization transfers a copy of its electronic records to NARA while retaining the legal custody and control over access to its records. The organization retains ownership of the records and must respond to discovery efforts like Freedom of Information requests until legal custody is conveyed to NARA. The pre-accessioning of records allows NARA to ensure the long-term preservation of permanent electronic records, and helps the organization mitigate the possibility of potential loss of its permanent electronic records. Information on the pre-accessioning process is available at http://www.archives.gov/research/electronic-records/info-for-archivists.html.

5. TRANSFER OF PERMANENT ELECTRONIC RECORDS. The office with ownership of the permanent electronic records should coordinate with the following components to ensure the records are transferred to NARA according to the requirements found in Title 36 Code of Federal Regulations (CFR) 1228, Subpart L [36 CFR 1228.270]:

a. Program Records Official (PRO)

b. DOE Records Management Program

c. Information technology support staff

d. NARA Center for Electronic Records (CER)

e. History Division (ME-75)

6. ACCEPTABLE MEDIA AND FORMATS FOR TRANSFERRING RECORDS.

a. Media. NARA accepts different media for transferring records, although it is often easiest and best for organizations to transfer their records on Compact-Disk, Read Only Memory (CD-ROM). Other acceptable media are magnetic tape and tape cartridges, such as Digital Linear Tape (DLT). File Transfer Protocol (FTP) may also be used.

b. Format. The format depends upon the type of records being transferred. Generally, they are:

(1) Textual records – NARA accepts plain ASCII or in Portable Document Format (PDF) or scanned images. More information on transferring textual records can be found at http://www.archives.gov/records-mgmt/initiatives/pdf-records.html; http://www.archives.gov/records-mgmt/initiatives/scanned-textual.html;

(2) Scanned images of textual records – NARA's preferred formats are Tagged Image File Format (TIFF) and Portable Network Graphics (PNG). Graphics Interchange Format (GIF) and Basic Image Interchange Format are also acceptable.

(3) Data files and databases – Data files and databases require more extensive documentation than other electronic records, and a record layout and codes are required for each file. NARA accepts tables that have been converted to files with fixed-length fields or fields defined by delimiters

(4) Digital geospatial data – NARA currently prefers Spatial Data Transfer Standard (SDTS) or Geography Markup Language (GML). More information on transferring digital geospatial data can be found at: http://www.archives.gov/records-mgmt/initiatives/digital-geospatial-data-records.html

(5) Digital photographic records – NARA prefers Tagged Image File Format (TIFF) or the highest resolution, uncompressed or modified raw file format the camera can produce. File Interchange Format (JFIF, JPEG) is also acceptable. More information on transferring digital photographic records can be found at http://www.archives.gov/records-mgmt/initiatives/digital-photo-records.html

(6) Web records – NARA accepts Hypertext Markup Language (HTML) and other formats such as TIFF or PDF that either are embedded in the HTML or

referenced by it. http://www.archives.gov/records-mgmt/initiatives/web-content-records.html

(7) E-Mail records http://www.archives.gov/records-mgmt/initiatives/email-attachments.html

7. PREPARING ELECTRONIC RECORDS FOR TRANSFER TO NARA. Background information should be collected before beginning the transfer process as follows:

a. Review the appropriate records disposition schedule for information on how and when the records are to be transferred.

(1) Review the NARA requirements for electronic records management at Title 36 Code of Federal Regulations (CFR) 1234, [36 CFR 1234].

(2) Determine if there are any special restrictions on the information; for example, National Security Information (NSI), confidential business information (CBI), or information subject to the Privacy Act.

(3) Identify the DOE IT staff person who will assist with the transfer.

b. Contact the RLO to begin coordination with NARA for the pending transfer of electronic records.

c. Prepare the records for transfer according to the requirement provided in Title 36 Code of Federal Regulations (CFR) 1228, Subpart L [36 CFR 1228.270]. In addition to the formats specified in the CFR, NARA also accepts other formats, such as Portable Document Format (PDF) files, scanned images, digital photographs, and Web content.

d. Assemble technical documentation that provides information on how the system captures, manipulates, and outputs data. Adequate documentation contains enough information to allow the records to be interpreted and understood in context. Documentation may be in the form of publications, administrative reports, user notes, system guides, file descriptions, Privacy Act notices, or manual or automated data dictionaries. NARA prefers the documentation in electronic format, but if that is unavailable, a complete, hard-copy set should be sent with the data.

e. Complete the following documents:

(1) Standard Form 258 (SF 258), "Agreement to Transfer Records to the National Archives of the United States"

(2) National Archives Form 14097, "Technical Description for Transfer of Electronic Records to the National Archives."

(3) Prepare a list of files corresponding with what is contained on the transfer media (e.g., tapes, cartridges, disks).

f. Distribute the completed paperwork as follows:

(1) Original and one copy of the SF 258, NA 14097, and the file list to the DOE Records Officer (IM-11) for signature. The DOE Records Officer will forward the original SF 258 package to NARA and retain the copy.

(2) One copy of the SF 258, NA 14097, and the file list to the appropriate PRO.

(3) Retain one copy of the complete SF 258 package, including the data and documentation, until NARA has approved the transfer.

g. Once NARA has approved the transfer, the DOE Records Officer will forward a copy of the signed SF 258 to the records custodian and the PRO. The records custodian will make arrangements for the records to be shipped to NARA.

h. Complete information about NARA regulations for transferring records can be found at: http://www.archives.gov/records-mgmt/initiatives/transfer-records-to-nara.html

CHAPTER X. IMAGING SYSTEMS

1. INTRODUCTION

Digital imaging is defined as the ability to capture, store, retrieve, display, process and communicate or disseminate records electronically using a variety of hardware and software components. Digital imaging technology continues to change at a rapid pace, but with the proper planning and controls, organizations can significantly improve its business operations without endangering processes through technology obsolescence.

2. BACKGROUND

Imaging is a process by which a document (primarily on paper, although any medium can be used) is converted from a human-readable format to a computer-readable digital image file. A digital image consists of pixels (picture elements or tonal values in binary code) arranged in columns or row. The number of pixels per inch determines the image's resolution (clarity and definition of the image expressed by width in pixels for image files or as dotes per square inch (dpi) for prints).

These imaged pictures of documents can be stored on a variety of media. The most common types of storage are magnetic media (such as tapes, disks, and magnetic cartridges) or optical media (such as CD-ROM and other removable disks known as "platters"), or on network drives. When combined with effective indexing, imaging the files can shorten information retrieval time and allow access to materials for multiple users at various locations.

To date, NARA has not developed requirements specifically for images. However, requirements for electronic records have been established in 36 CFR Part 1234; audit trails to serve as the record that the images were created properly and validated must be maintained [similar to the steps required for microfilm records in 36 CFR 1230.12(a)-(c).]

2. CREATION OF IMAGES

a. Images must contain all information shown on the originals.

b. Images must be able to be used for the purposes the original records served.

c. Procedures must be created and audit trails provided to serve as a record that the images were created properly and validated.

d. A migration plan must be developed to ensure that the information in the images can be accessed throughout the entire retention period of the records. NARA must approve retention periods.

e. The imaging system must meet the requirements for security as outlined in Chapter II, section 4 of this Manual.

e. For new or proposed imaging systems, a cost-benefit analysis should be completed before choosing to implement any imaging system.

3. DISPOSITION OF RECORD IMAGES

a. Temporary Records. .

(1) Imaged copies of records already scheduled as temporary do not need to be rescheduled if the nature and content of the records remain identical to the description in the schedule.

(2) Apply the disposition authority approved by NARA for the paper records

(3) Retention of the paper copies after imaged copies have been verified adds costs by requiring organization of the files, periodic file cutoffs, and retirement to a records storage facility or disposal and should be avoided..

b. Unscheduled Records. When unscheduled records are imaged, the image file and the paper records must both be scheduled and the paper copies may not be disposed of until an approved schedule covering the records is approved. The schedule should provide for the disposition of both the paper and imaged copies and specify which version is the recordkeeping copy.

c. Permanent Records. When paper records that are scheduled as permanent are imaged, the imaged files must also be scheduled. The organization must not dispose of the paper until NARA has approved a new schedule for them. The schedule should provide the disposition of both the paper and imaged copies and specify which is the recordkeeping copy.

4. FACTORS TO CONSIDER. There are advantages to instituting imaging systems, such as increased storage capability, elimination of "out-of-file" problems, shortened retrieval times, improved retrieval by multiple users, and ease of information dissemination.

There are also disadvantages such as expensive hardware and resource-intensive indexing requirements, as well as rapid technological changes that require frequent upgrades of hardware

and software. Migration and conversion of records in imaged format may also be needed to protection the information in records not eligible for disposal.

ATTACHMENT 1: DOE DEPARTMENTAL ELEMENTS, AND BY AGREEMENT, THE NATIONAL NUCLEAR SECURITY ADMINISTRATION, TO WHICH DOE M XXX.X-X IS APPLICABLE[1]

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Independent Oversight and Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Management, Budget and Evaluation and Chief Financial Officer
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Secretary of Energy Advisory Board
Office of Security
Office of Security and Safety Performance Assurance
Office of Legacy Management

[1]Field entities should not to be listed unless there are special circumstances necessitating their inclusion. Applicability to a field entity is assumed when its lead program Secretarial Officer organization is listed.

Bonneville Power Administration[2]
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

[2]All Manuals should address whether the Bonneville Power Administration (BPA) and other organizational elements are covered. BPA is currently exempt from a number of DOE directives. However, for any directive issued after September 27, 2002, including new directives and revisions of existing directives, the Department may reevaluate whether BPA should be covered. Accordingly, any new or revised Manual should specify whether or not BPA is covered.

ATTACHMENT 2 - CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) contractors, including National Nuclear Security Administration (NNSA) contractors, who create, use, maintain, receive, disseminate, or dispose of DOE electronic records in connection with the performance of DOE-funded tasks of activities. Contractors must comply with the following requirements.

Regardless of the performer of the work, the contractor is responsible for complying with the requirements of this CRD. The contractor is responsible for flowing down the requirements of this CRD to subcontractors at any tier to the extent necessary to ensure contractor compliance with the requirements.

In addition to the CRD in DOE O 241.1, Records Management Program, and as directed by the Contracting Officer, the contractor must do the following:

1. GENERAL REQUIREMENTS.

   a. Assign responsibility to develop and implement a contractor program for the management of all records created, received, maintained, used, or stored on electronic media and notify the Contracting Officer of the name and title of the person assigned the responsibility.

   b. Integrate the management of electronic records with other records and information resources management contractor programs.

   c. Incorporate electronic records management objectives, responsibilities, and authorities in pertinent contractor policies and procedures.

   d. Establish procedures for addressing records management requirements, including recordkeeping requirements and disposition, before approving new electronic information systems or enhancements to existing systems.

   e. Ensure adequate training is provided for users of electronic mail systems on recordkeeping requirements, the distinction between Federal records and nonrecord materials, procedures for designating Federal records, and moving or copying records for inclusion in the contractor's recordkeeping system.

f. Ensure that adequate training is provided for users of electronic information systems in the operation, care, and handling of the equipment, software, and media used in the system.

g. Developing and maintaining up-to-date documentation about all electronic information systems that is adequate to: Specify all technical characteristics necessary for reading or processing the records; identify all defined inputs and outputs of the system; define the contents of the files and records; determine restrictions on access and use; understand the purpose(s) and function(s) of the system; describe update cycles or conditions and roles for adding information to the system, changing information in it, or deleting information; and ensure the timely authorized disposition of the records.

h. Specifying the location, manner, and media in which electronic records will be maintained to meet operational and archival requirements, and maintaining inventories of electronic information systems to facilitate disposition.

i. Specifying the methods of implementing controls over national security-classified, sensitive, proprietary, and Privacy Act records stored and used electronically.

j. Reviewing electronic systems periodically for conformance to established procedures, standards and policies as part of the periodic reviews required by 44 U.S.C. 3506. Implement a records management program in compliance with requirements for managing records in all formats, including early capture and control throughout their life cycles.